Axellio - Pioneering Threat Detection and Response

Axellio provides complete solutions for security threat detection and response from its base platform PacketXpress to vertically integrated, end-to-end solutions as well as consulting and professional services. Axellio offers a comprehensive portfolio designed for security work-flow efficiency and cost-effectiveness optimized for your team, environment, and security objectives.

Most companies' security posture is still centered around a castle mentality – secure the ingress and egress of your network and the end-devices to keep threats out. This approach leaves organizations vulnerable as 34% of security threats are internal to the organization[1], either through intentional or unintentional actions of employees and partners or dormant malware already present in the network. And once attackers are inside your network, it is extremely difficult to detect them, giving them time to uncover valuable assets while moving laterally throughout your network undetected and potentially exfiltrating critical information.

To make matters worse, today's threat detection and response are still based on a traditional approach of real-time analysis of traffic data and device logs, extracting key metrics, and storing those as meta-data. This data may be sufficient for early indicators and dashboards for most threats but are often insufficient to answer the critical questions required to ensure better mitigation: what happened before and after the reported event?

Axellio's innovative new approach addresses those critical issues of

- Gaining visibility into your internal, East-West network to detect internal threats
- Obtaining access to packets surrounding any event as unalterable evidence
- While taking advantage of your existing security infrastructure.

Axellio's goal is to leverage the resources and tools you already have in place while providing faster access to richer, more contextual data. This allows you to prioritize what matters, for rapid and informed decisions, and for efficient response across your entire threat lifecycle: from threat detection over alert triage and incident response to threat hunting.

This ensures you maximize the value of your existing environment while reducing Mean-Time-to-Detect (MTTD) and Mean-Time-to-Respond (MTTR).

A Total Solution for Threat Detection and Response Optimized for Your Environment

Axellio has developed an approach to optimize a solution fit for your environment to prevent tool and data overload:

1. Jointly perform an assessment of your security posture, focusing on people, processes, and technologies to align the solution with your strategy and identify the gaps in your approach.
2. Design, engineer, and implement an economical solution focusing on efficiency and coverage based on your needs: leveraging & optimizing your current infrastructure, enhanced with the Axellio platform as necessary, utilizing Open-Source solutions where applicable.
3. Make it work for your team and processes to ensure you maximize your investment by working closely with you to deploy, configure, document, and educate your team.

[1] Source: 2019 Data Breach Investigations Report, Verizon

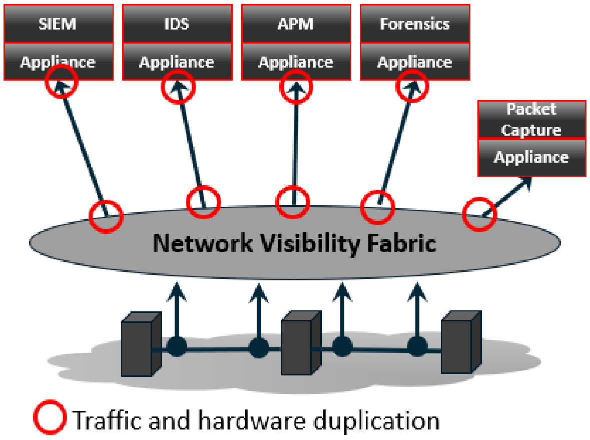
Today’s Approach - Efficient but Leaving Organizations Vulnerable

Today’s network analysis for security, such as an Intrusion Detection System (IDS) or Network Detection and Response (NDR) systems are complex, costly, and difficult to manage. This has led many organizations to limit their monitoring only to high-aggregation points, especially network ingress and egress (North-South) interfaces which accounts for only 15% of the total enterprise traffic[2]. This lack of visibility leaves organizations vulnerable to insider threats, as a staggering 34% of all threats come from within internal networks[3].

Most traditional monitoring applications are based on the same approach. They are optimized for threat detection but are frequently insufficient for incident analysis and response:

1. Traffic is collected and analyzed in real-time and vital performance and event information is extracted.
2. The results are stored in metadata records, which can be efficiently stored.
3. Packets are discarded, or only select ones are kept for future reference.

The need to analyze all traffic in real-time results in a highly compute-intensive solution, with many of those products utilizing proprietary hardware to optimize processing and storage. To keep up with ever-increasing network speeds and volume often requires traffic distribution across multiple appliances, fed by sophisticated Packet Brokers as part of the Network Visibility Fabric (NFV) to filter, group, and allocate traffic flows to the right monitoring instance. With each application appliance being purpose-built, any additional analysis of the same traffic (e.g., one for security, the other for application performance) requires the same hardware-intensive set-up, traffic duplication, and additional network, processing, and storage infrastructure.



This environment makes it complicated, costly, and tough to manage and to upgrade infrastructure:

- Each application has its dedicated appliances to process traffic in real-time.
- The same traffic needs to be duplicated and processed by multiple applications for different purposes
- The entire infrastructure needs to be designed for peak traffic – as anything less will lead to overload situations resulting in information loss.
- With traffic growing at double-digit rates annually[4], upgrading this entire infrastructure is resource-intensive and complex.
- The resulting metadata is still incomplete for getting to the root cause
- Access to packets is often reactive and incomplete if available at all for back-in-time forensic and root-cause analysis, pre-and post-event.

[2] Cisco’s Global Cloud Index 2019
[3] Verizon: 2019 Data Breach Investigations Report, Verizon
[4] EMA: Network Management Megatrends 2020

Streamlining Threat Detection and Response through Packet Data

Over the last decade, the industry has settled on making decisions on mostly meta-data as this information is readily available and can be easily stored. Despite that capturing the actual traffic in form of packets provides a much richer set of data, it has been dismissed as too complex and expensive and is only employed sparingly. This leaves many organizations with the below data which is overwhelming in volume but often insufficient for rapid incidents response:

- NetFlow and the Internet Protocol Flow Information Export (IPFIX) traffic flow information
- An overwhelming amount of log data from any device in the network
- Events and alarms created by distributed analysis applications such as EDRs, IDSs, etc.

Threat actors are taking advantage of this approach by concealing their activity from the security team:

- Hiding their activity within perfectly legitimate traffic by properly encoding the packet header information as most network traffic analysis applications only analyze the protocol headers. They even go so far as to spoof application-specific header information to fool Deep Packet Inspection solutions.
- Hackers are checking on the presence of end-point protection before taking any malicious action, avoiding those that are heavily protected and targeting less protected devices.
- Advanced threat actors typically design their tools to remove trace evidence or even modify logs or files from victim machines to hide their malicious activities.
- Camouflaging the attackers real intend with simultaneous Denial of Service (DOS) attacks that overwhelm the security monitoring infrastructure, leading to packet loss and allow the intrusion to go undetected.

Capturing and analyzing network packets surrounding the attack are immutable evidence as they are nearly impossible for attackers to delete or modify. Attackers still need to correctly encode packets to pass through the network and ensure they contain the right information for the action they intend to illicit. When captured, this provides a rich data set that can be analyzed pre-and post-event to determine how attackers entered the environment, what actions they took, and which devices were communicated with:

- Packets can reliably recreate all communication relationships to assess the “blast radius.”
- Allows for analysis of not just the header information but all payload embedded in the packets
- Provide reliable timing information on all packets traversing the network
- Provide broader attack patterns across multiple devices

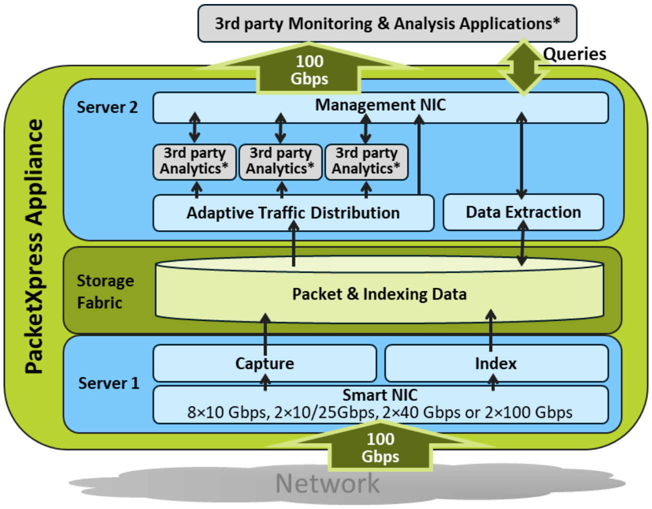
Packets provide a rich set of unalterable information and the solid foundation needed for quick threat response.

Solution Brief

Threat Detection and Response

Axellio PacketXpress^{TM} - the Network Visibility Hub

Rethinking Network Traffic Analysis



Using the latest storage and server architecture technologies available, Axellio developed a high-speed, high-intake network visibility hub for packet capture, analysis, and distribution in an extremely small footprint. As PacketXpress buffers the incoming traffic, it removes the real-time processing requirement. This allows the monitoring and analysis applications to turn into software-defined solutions, virtualizing the previously hardware centric approach while storing all packets.

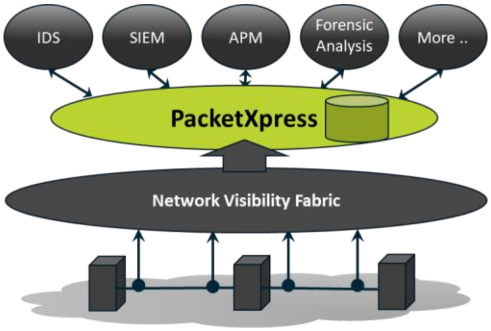
Axellio PacketXpress is a dual-server architecture platform which can ingest, store, and distribute traffic simultaneously at 100 Gbps inbound and outbound with no performance impact on either intake, distribution, or analysis. Axellio combined technology previously requiring an entire rack of equipment into a 3U high (equal to 5¼ inches) rackmountable solution by leveraging leading-edge server and storage technologies and developing a new, innovative file system. Using common, off-the-shelf components (COTS) reduces maintenance and procurement costs.

- PacketXpress allows for ingest rates reliably without packet loss for up to 100 Gbps with bursts up to 200 Gbps and is not impacted by how much data is read from disk by dedicating Server 1 completely to capture, indexing, and storage. Hardware-based traffic filtering, deduplication, and slicing can reduce the amount of traffic being captured.
- The storage consists of NVMe SSD drives with a raw storage capacity of up to 1.5 Peta Bytes. This unique approach of a high-density dual-server architecture combined with flexible PCIe lane switching to dual ported NVMe SSD drives using Axellio's proprietary file system attains the high performance in read/write required. This allows both servers to access information simultaneously on the same storage media, without impacting either read or write actions from either server.
  The option for compression of on-disk packet data can further decrease the storage space required thus reducing the upfront cost of the solution while increasing the amount of time you can store packets for later retrieval. Additionally, PacketXpress provides long-term archival solutions for extended storage at reduced cost.
- Server 2 is designed for data extraction, analysis, and distribution, all at rates up to 100 Gbps without impacting the data intake or storage performance. Multiple data extraction streams can be individually configured for the maximum bandwidth the application can consume. Each stream allows to define its traffic content based on a 5-tuple configuration (source/destination address, protocol, and port number) or using the rich filter capabilities of the Berkeley Packet Filter (BPF). Due to its ability to access on-disk packets without reducing intake performance, PacketXpress allows for dynamic queries without the need to pre-define indexing at time of capture, offering more flexible and dynamic analysis capabilities.
- Using standard software APIs such as PFRing or libpcap, analysis applications can either be hosted on the server directly, or traffic can be forwarded to off-box applications in either physical or virtual environments.

- As data can be stored anywhere from minutes to weeks or even longer, access to any packet data for post-event analysis for threat hunting and forensic analysis is readily available, using standard PCAP analysis tools. This provides the flexibility to obtain historical pre-and post-event data on demand from any event reported on another application. Using flexible BPF filter capabilities that do not rely on indexing at time of intake provides the flexibility needed to analyze based on any packet data.

PacketXpress - An Open Platform Delivering the Complete Solution

PacketXpress is an application agnostic, open platform supporting many APIs to integrate with your current solutions to protect your existing investment and avoid costly ramp-up times and process changes.



With PacketXpress inserted between the network visibility fabric responsible for collecting, aggregating, and filtering traffic and your existing monitoring applications, you can leverage the monitoring infrastructure already in place. This applies to all applications, whether operating in physical or virtual platforms.

Being able to pivot directly from an event drives faster decisions on whether an event is urgent and important by direct access to complete pre-and post-event packet data with a click of a button, avoiding lengthy data collection and correlation. This allows the efficient filtering out of false positives and lower priority events while focusing on imminent threats that have progressed further down the kill chain.

All applications consuming packet data benefit from PacketXpress being able to buffer traffic spikes and the occasional traffic growth. PacketXpress can smooth out traffic spikes that otherwise overload applications and lead to information loss due to its store and forward approach. As an added economic advantage, instead of sizing applications for peak traffic rates, applications can now consume traffic at the average rate, using fewer resources and delaying required capacity upgrades. If upgrades are needed, applications can now be virtualized and spun up or down depending on the analysis load, utilizing PacketXpress' software APIs.

Axellio frequently utilizes open-source solutions to close analysis gaps and to keep costs under control. The below list provides a selection of open-source security applications Axellio has successfully integrated into the platform:

Area	Open-Source Solution Examples
Network Traffic visibility	• NIDS: Suricata • Traffic analysis and classification: Zeek • File Extraction: Strelka
Host visibility	• HIDS: Wazuh • Analysis: Osquery – SQL queries
Logs	• Store: Elasticsearch, Redis • Monitor: ElastAlert • Analyze: Community ID • Manage: Curator, Data Fields, Re-Indexing
Collect	• Logstash, Ingest, Filebeat, and others
Analyze	• ElasticSearch: Kibana, Hunt • ATT&CK Maaping: ATT&CK Navigator • Packet Analysis: NetworkMiner, Wireshark, Downloads • Host analysis: Fleet • Data management: CyberChef
Respond	• Incident Response Platform - TheHive • Detection Playbook – Playbook

We are always open integrating other solutions depending on your needs and technologies as well.

Beyond Detection and Response – Getting the Most of Your Investment

PacketXpress also provides benefits beyond threat detection and response:

- **Mitigation validation –** After implementing the mitigation or fix, it is essential to validate whether the issue has been resolved. Given the complexity of today's networks, simulations are often difficult to generate. And without the original traffic data pre-and post-event, a validation of the fix is challenging at best. Having the actual packet data available for any event allows you to replay traffic to validate that the mitigation or fix has resolved the issue. Furthermore, those can be made available for DevOps to test future developments with.
- **Training and education** – Replaying the captured attack traffic for training purposes creates realistic scenarios based on actual events, allowing faster dissemination of knowledge across the organization.

PacketXpress Data Sheet

The following outlines the PacketXpress flagship version.
Lower speed and capacity platforms are available as needed.

PacketXpress Appliance	
Network Connectivity	• Inline or Tap/Span port connect • Ethernet connectivity for up to: 8×10 Gbps, 2×10/25Gbps, 2×40 Gbps or 2×100 Gbps • Tunneling: GTP, IP-in-IP, GRE and NVGRE
Hardware Accelerated	• Zero packet loss for all frame sizes (including Jumbos) • Filtering: L2 - L4 with stateful flow management • Deduplication, slicing (fixed or dynamic offset), multi-port packet merge, IP fragment handling
Time Sync	• IEEE 1588-2008 PTP and PPS – PCAP and UNIX • 1 ns time stamp resolution
Storage	• Up to 1.5 Peta bytes via 48 hot-swappable Solid-State Drives (SSD)
Distribution Connectivity	• Up to 16 streams of up to 100 Gbps adaptive traffic distribution to feed external applications across different interface configurations
Processing	• 20 Million IOPS, 240 GBps system throughput • Two servers per chassis each with two Intel Xeon Cascade Lake Servers: up to 56 cores/112 threads per server, up to 2TB of RAM
Extensible	• Additional PCIe slots for GPUs, for NVMe SSDs, or other PCIe cards
Formfactor	• 3U high, 30 inch deep for Industry Standard Rack mounting • N+2 Redundant power supply

Contact us

For additional information please contact us at:

🌐 **https://axellio.com/**

✉ **contactus@axellio.com**

☎ **1 (800) 463-0297**
1 (719) 309-3370

The above specifications are based on the configuration supported as of the date of the publication and may change without notice. Axellio shall not be liable for technical or editorial errors or omissions contained herein. Please contact us for the latest information.